

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kenneth Jay Hurst, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

Introduction

1. I have been employed as a Special Agent of the Federal Bureau of Investigation ("FBI") since 2016, and am currently assigned to the Cincinnati Division. I entered on duty as a Special Agent in 2016 and am currently assigned to the Complex Financial Crimes Squad of the Cincinnati Division. In this capacity, I investigate matters involving criminal enterprises, white collar crimes, civil rights violations, bank robberies and the online exploitation of children. Prior to my current assignment, I was assigned to a Counterintelligence Squad, where I investigated a wide array of national security matters. Since 2016, I have received training and investigative experience in interviewing and interrogation techniques, arrest procedures, search and seizure, search warrant applications, and various other crimes and investigative techniques including Title III investigations.

2. Prior to my employment as a Special Agent with the FBI, I was a Captain in the United States Army in a reconnaissance and surveillance organization. In that capacity, I conducted numerous interviews and interrogations while deployed to Afghanistan in 2014. Prior to my career in the United States Army, I was a full time student. I graduated from the University of Kentucky in 2012 with a Bachelor's Degree in International Studies.

3. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

4. I am investigating the activities involving the sexual abuse of a minor and the corresponding production of images memorializing the sexual abuse that occurred at 10651

South State Route 48, Loveland, Ohio 45140. As will be shown below, there is probable cause to believe that evidence involving the sexual abuse of a minor and corresponding production of images memorializing the sexual abuse will be located at 10651 South State Route 48, Loveland, Ohio 45140. I submit this application and affidavit in support of a search warrant authorizing the search of the above residence ("Premise"), as further described in Attachment A-1, as well as mobile telephones provided to the Hamilton Township Police Department ("HTPD"), via Consent to Search Forms ("Subject iPhone" and "Witness iPhone"), as further described in Attachments A-2 and A-3. Located within the Premises, Subject iPhone and Witness iPhone to be searched, I seek to seize evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing production and possession of child pornography, more particularly described in Attachment B. I request authority to search the entire premises, including the residential dwelling, outbuildings, and vehicles on the premises, and any computer and computer media located therein, as well as the Subject iPhone and Witness iPhone, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of a crime.

5. The statements in this affidavit are based in part on information provided by HTPD and on my own investigations of this matter, including my experience and training as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of §§ 2251, 2252 and 2252A, are presently located at the premises.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252 and 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2251(a) prohibits knowingly producing a visual depiction of a minor engaged in sexually explicit conduct, using materials that affect interstate commerce.

b. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

c. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

d. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.

e. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.

h. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means any material in a manner that reflects the belief or is intended to cause another to believe that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

i. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

- a. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. “Child Pornography” includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).
- c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).
- d. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to,

central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. “Peer-to-peer file-sharing” (“P2P”) is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user’s computer, and conducting searches for files that are currently being shared on another user’s computer.

k. “Sexually explicit conduct” applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

l. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

m. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as

well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced, distributed and stored.

9. Computers and cellphones basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking. The term computer in this affidavit should be read to include cellphones.

10. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers and cellphones around the world. Indeed, modern day cellphones have many of the same capabilities as computers. Many cellphones now have digital cameras as well.

11. The computer and cellphones ability to store images in digital form make them ideal repositories for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers and cellphones has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords individuals several different venues for meeting each other, obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Apple, Google, Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer and instant messaging software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard

drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

15. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process

can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

16. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

17. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF THE INVESTIGATION

18. Your Affiant states that on November 20, 2017, the Hamilton Township Police Department (HTPD) received a witness report stating JAKE MICHAEL DAMRON had taken pornographic pictures of a five year old minor victim (hereinafter referred to as "MINOR VICTIM"). MINOR VICTIM is the daughter of DAMRON'S girlfriend, (hereinafter referred to as "GIRLFRIEND") with whom he resides. The witness reported DAMRON was trading the images of MINOR VICTIM for other child pornography via the cell phone application "KIK."¹

23. On November 21, 2017 a Detective with HTPD and a Warren County Children's Service Case Worker responded to DAMRON'S address, 10651 South State Route 48, Loveland, Ohio 45140 in an attempt to locate MINOR VICTIM and GIRLFRIEND. The detective found the residence to be unoccupied and contacted GIRLFRIEND via telephone. Arrangements were made to meet with GIRLFRIEND at the Warren County Child Advocacy Center. On November 21, 2017 at approximately 1420 hours, the detective interviewed GIRLFRIEND at the Advocacy center.

24. GIRLFRIEND advised on October 28, 2017, she became suspicious of DAMRON and searched his cell phone (Subject iPhone) while he was sleeping. GIRLFRIEND observed conversations in DAMRON'S cell phone between DAMRON and other individuals, which included several pictures of young female children including MINOR VICTIM. GIRLFRIEND used her personal cell phone (Witness iPhone) to take pictures of the images and conversations displayed on DAMRON'S cell phone and confronted DAMRON with the pictures. GIRLFRIEND advised she initially kicked DAMRON out of the house upon discovering the images and conversations, but allowed DAMRON to move back into the house approximately

¹. Kik is an internet based messaging and communication application which is usable on cellphones and other internet capable devices.

one week later, after DAMRON agreed to attend therapy. Sergeant Short subsequently requested that GIRLFRIEND respond to the Hamilton Township Police Department headquarters for further interviewing.

25. GIRLFRIEND immediately responded to HTPD where she voluntarily turned her cell phone over and provided her passcode. GIRLFRIEND also signed a property release form and a consent to search form. GIRLFRIEND then completed a three page voluntary written statement. In the statement, GIRLFRIEND advised she felt suspicious of DAMRON and searched his cell phone. During the search she found sex applications and chatrooms including the application "KIK." In "KIK," GIRLFRIEND found many conversations between DAMRON and other "KIK" users exchanging videos and images. The images in the conversations included pictures of GIRLFRIEND and MINOR VICTIM. Additionally, DAMRON had sent and received sexually explicit pictures of other children. GIRLFRIEND confronted DAMRON with the images and DAMRON apologized to GIRLFRIEND and told her that he knew what he had done was wrong. GIRLFRIEND then kicked DAMRON out of the house but continued to feed him and allow him to enter with permission. GIRLFRIEND advised she confided in friends and asked them for advice and also told MINOR VICTIM'S psychologist about the incident.

26. On November 21, 2017, at approximately 1640 hours, Sergeant Short conducted a non-custodial interview of DAMRON at the HTPD. On November 28, 2017, Your Affiant reviewed a video recording of the interview. The interview lasted approximately twenty-eight minutes and DAMRON provided the following information:

- DAMRON stated that he had "nude pictures of kids" on his phone and responded in the affirmative when asked by Sergeant Short if he had been sending and receiving them.

- DAMRON also advised he had taken inappropriate pictures of MINOR VICTIM.
- DAMRON had deleted all of the pictures off of his phone but possessed the cell phone.
- DAMRON identified his "KIK" username as "HITEMYOUNGIN" associated with the email address "cincityracer@yahoo.com".
- DAMRON deleted the account from his phone after being confronted by GIRLFRIEND but confirmed his account was still active.
- When asked by Sergeant Short if DAMRON had been trading child pornography on "KIK", DAMRON responded in the affirmative.

27. DAMRON consented to turning his iPhone 6s² cell phone over to Sergeant Short and agreed to provide his cell phone passcode. Sergeant Short advised DAMRON he would be analyzing the cell phone and would present the results to a Grand Jury. DAMRON again agreed to turn the phone over to Sergeant Short, he then signed a property release form and signed a consent to search form. DAMRON explained MINOR VICTIM was the only minor he had taken photographs of and stated he had "probably" taken them due to easy access. DAMRON also stated he is registered as a sex offender with the State of Ohio

28. On November 27, 2017 Your Affiant received the HTPD case file, interview notes, and DAMRON'S cell phone as well as GIRLFRIEND'S cell phone. Upon receiving GIRLFRIEND'S cell phone, a pink iPhone 6s, Your Affiant reviewed GIRLFRIEND'S signed and dated consent to search form. Upon verification of GIRLFRIEND'S consent to search, at approximately 1610 hours, Your Affiant turned GIRLFRIEND'S cell phone on, placed the device into airplane mode and reviewed GIRLFRIEND'S camera roll. Your Affiant identified

². From experience, I know iPhone cellphones are typically manufactured outside the United States.

multiple photographs taken on October 28, 2017, of a cell phone matching the description of DAMRON'S with conversations and images depicting what appeared to be shared photographs including the following:

- A prepubescent female straddling what appeared to be an erect male penis
- What appeared to be a prepubescent female naked spreading her legs.
- Photographs of what appeared to be an adult male hand pulling back underwear to expose the genitalia of what appeared to be an unidentifiable prepubescent female.

29. At approximately 1635 hours, Your Affiant concluded the review of the cell phone and powered the device off.

30. Public database records checks and Ohio Bureau of Motor Vehicles identified that DAMRON, date of birth XX-XX-1992, Social Security Account Number XXX-XX-3187, resides at 10651 South State Route 48, Loveland, Ohio 45140.

31. During his interview with Sergeant Short, DAMRON provided 10651 South State Route 48, Loveland, Ohio 45140, as his residential address.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE
DISTRIBUTION, TRANSPORTATION, RECEIPT, OR POSSESSION AND
ATTEMPTED DISTRIBUTION, TRANSPORTATION, RECEIPT, OR
POSSESSION OF CHILD PORNOGRAPHY**

32. As set forth above, probable cause exists to believe that DAMRON has produced, distributed, and possessed child pornography. Based upon my knowledge, experience, and training, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years

and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

33. DAMRON, residing at 10651 South State Route 48, Loveland, Ohio 45140, exhibits the common characteristics described above in ¶ 27 of someone involved in the distribution, transportation, receipt, and possession of child pornography, or the attempt to distribute, transport, receive, or possess child pornography, is evidenced by the facts that are set forth in this affidavit, including:


a. The fact that sexually explicit images of MINOR VICTIM were produced to document the abuse and preserve the abuse for later review and sexual gratification;

- b. The sexually explicit images of MINOR VICTIM were produced using a mobile device, allowing for the contents to be kept in digital format, and easily transported, distributed, and stored.
- c. DAMRON's own statements of producing, distributing, receiving, and possessing child pornography.

CONCLUSION

34. Based on the aforementioned factual information, Your Affiant respectfully submits that there is probable cause to believe that evidence of the above described sexual abuse, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A, will be located at the residence associated with DAMRON, as well as both the Subject iPhone and Witness iPhone. Additionally, the evidence listed to be seized, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

35. Your Affiant, therefore, respectfully requests that the attached warrants be issued authorizing the search and seizure of the items listed in Attachment B.


Kenneth Jay Hurst
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 29 day of November, 2017.


HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-2

DESCRIPTION OF THE SUBJECT IPHONE TO BE SEARCHED

An Apple iPhone 6S, silver in color, Model A1688, FCC ID: BCG-E2946A IC: 579C-E2946A. The iPhone was turned over to HTPD by DAMRON with consent to search and is being stored at the FBI Cincinnati Field Office, 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236.

ATTACHMENT B

PROPERTY AND PARTICULAR ITEMS TO BE SEARCHED AND SEIZED

Agents are authorized to photograph or video the interior and exterior of the building. Additionally, all items contained in the premises described in Attachment A-1, A-2, and A-3 that relate to violations of 18 U.S.C. §§ 2251, 2252 and 2252A, relating to the production, distribution, transportation, receipt, and possession of child pornography:

1. Child pornography or child erotica in any format or medium;
2. Girl's clothing, including underwear and similar clothing items;
3. Sexual toys and items used for sexual arousal or sexual acts;
4. Any computer or storage medium, including but not limited to, computers, computer servers, cellular telephones, personal data assistants, tablets, electronic storage devices, thumb drives, flash drives or cards, and smart cellular telephones;
5. Any images of Minor Victim;
6. Any information, communications, images, videos, messages, or data associated with Kik messenger;
7. Records and information relating to the identity or location of the suspects, or others who may have communicated with for the purpose of exchanging and/or trading images of minors;
8. Computers or storage media used as a means to commit the violations of 18 U.S.C. §§ 2251, 2252 and 2252A;
9. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

- web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.
10. Routers, modems, and network equipment used to connect computers to the Internet.
11. All visual depictions in any form, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct and any mechanism used for the receipt, storage, or production of the same.
12. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, data, or documentation. Data security devices may consist of hardware, software, or other programming code.
13. Any and all documents, records, e-mail, and internet history (in electronic form) pertaining to the sexual exploitation of children whether transmitted or received.
14. Any and all electronic records, documents, invoices, notes, and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found at that property.
15. Electronic or paper documents and records regarding the lease and/or possession or ownership of the property described in Attachment A-1, A-2, or A-3 or of any computer or electronic storage device found at that property.
16. Evidence of user attribution showing who used or owned any of the items seized under this warrant, including evidence of when those items were created, edited, or

deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

17. Records evidencing the use of the Internet, to include Internet Protocol addresses including:
 - a. records of Internet Protocol addresses used;
 - b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
18. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
19. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
20. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
21. Any images or videos that depict Minor Victim.
22. Any communications with or about Minor Victim.

23. Any text, email, or other communication concerning the sexual exploitation of children.
24. Any hotel records and receipts, travel records and receipts, vehicle records, financial records, and telephone bills.
25. Any record, receipt, or advertisement pertaining to sexual exploitation of minors.